WHITEPAPER

Understand how SSO and MFA improve security

IT departments today get squeezed from all sides. Budgets are tight, compliance requirements large, and IT is tasked with keeping the organization secure while enabling employees, contingent workers, gig workers, vendors, and partners to work productively in a globally distributed ecosystem.

Competition is fierce today, so businesses and organizations have to stay agile, keep transforming themselves, and be able to implement new procedures, systems, and software quickly. Acquisitions, mergers, and a constantly churning workforce don't make it any easier.

Whether at a desk, on a tablet, or using a mobile phone, employees expect fast access to company resources. At the same time, you can't compromise on security.

IT departments are expected to onboard and offboard users quickly and provide them easy access to the applications and resources they need—all while maintaining the highest levels of security. And today's workforce requires constant access via a wide variety of devices: laptops, tablets, and mobile phones.

Failure to adequately protect against data breaches can lose your company clearances, IP, lawsuits, and customers.

Accommodating all these requirements is a monumental job. The IT department plays a pivotal role in achieving it.

Security is costly—but a breach is even more so

According to the SANS Institute[1], 42% percent of surveyed IT professionals said their endpoints had been breached. And while the year 2017 was a high-water mark for breaches, 2018 wasn't far behind.[2]

In fact, the risk of a breach just keeps growing, especially as new devices proliferate. 82% of senior IT professionals predicted that unsecured IoT devices would cause a data breach in their organization, with 80% saying such a breach could be catastrophic.[3]

DATA BREACH ARE DEFINITELY COSTLY:

- From a pure dollar perspective, the per-capita cost for breaches has risen to $148, according to IBM and Ponemon.[4]
- The average cost of a breach is $3.86 million worldwide and $7.91 million in the United States.

[1] "Industries Were Mergers and Acquisitions are Most Common," Investopedia, Nov 15, 2018 and "Number of merger and acquisition deals in the United States in the third quarter of 2018, by industry," Statista, 2018

[2] https://www.riskbasedsecurity.com/2018/08/over-2300-data-breaches-disclosed-so-far-in-2018-exposing-over-2- 6-billion-records/

[3] "Cost of a Data Breach Study," IBM and Ponemon, 2018.

- In the United States, the cost of lost business from breaches was $4.2 million. The largest breaches (50 million records or more) resulted in up to a $118 million loss.

- Lost business mainly comes from customer turnover, since 75 percent of consumers say they won't do business with companies that they can't trust with their data.[5]

Along with losing customers, another big impact for businesses is lost intellectual property (IP). Losing IP or trade secrets can create an existential threat, but even if a competitor doesn't use the knowledge to undercut the market, it can take a long time for a company to recover.

For example, in 2011, an employee stole and sold source code from American Superconductor (AMSC). The impact for AMSC was enormous, with its stock price devastated and its market value reduced by about $1.4 billion. It had to cut its workforce by 70 percent and relocate its headquarters to save money.[6]

That's one reason that regulations and requirements placed on organizations and companies are focused on access.

Protection costs. But failing to protect your data and IP costs more. Recent security breaches show what's at stake:[7]

- Apple discovered malware that had obtained sensitive information for 225,000 iPhone users.
- In a recent Facebook breach, the information of 50 million users was exposed.
- In 2016, 57 million Uber customer records were stolen by hackers.

For all these reasons, investing in technology and procedures to protect your organization and customer data is money well spent.

Failure to adequately protect against data breaches can lose your company clearances, IP, lawsuits, and customers.

The impact of breaches is lasting. Breached companies underperformed the NASDAQ by -3.7% after one year and -15.58% after three years.

Passwords are the weakest link

Regulatory legislation such as Sarbanes-Oxley (SOX) imposes requirements on information security, data access, as well as segregation of duties (SOD) policies. These requirements include mature processes for access certifications and policy management to make certain policies are in place and adhered to.

It's no surprise that passwords are a focus for compliance and IT departments—they're a focus for hackers, too. The most common attacks are aimed at obtaining user credentials, with the password being the critical element. That includes attacks like:

- **Phishing.** The attacker uses a list of phone numbers or email addresses and delivers a message with a compelling call to action that sends users to a fake website where they provide their username and password.

[5] "New Survey Finds Deep Consumer Anxiety over Data Privacy and Security," IBM/Harris poll press release, April 16, 2018.

[6] "The Unreal Scope of China's Intellectual Property Theft" The American Conservative, July 23, 2018.

[7] "The hacks that left us exposed in 2017" CCN, Dec. 20, 2017

- **Spear phishing.** The attacker targets a small group of individuals using well-crafted, believable messages that are relevant to the target group, often with personalized content. Again, a call to action gets users to provide their credentials.

- **Keylogger.** The attacker installs a program (often via a virus) that captures every keystroke on the user's computer, including sites visited, usernames, passwords, answers to security questions, and more.

- **Credential stuffing.** The attacker uses stolen credential pairs for one site on other sites, trying to gain access to many different sites.

- **Brute force and reverse brute force.** The attacker uses a program to generate possible username/password combinations to gain access. Or the attacker tries the most commonly used passwords (like Password123) on many different accounts.

- **Man-in-the-middle (MITM).** The attacker's program inserts itself into the interaction between a user and an app. The program then gathers the login credentials that the user enters—or even hijacks the session token.

Weak memories and too many passwords exacerbate the problem

Many of these attacks rely on the fact that users have to login to too many sites using different passwords. So they tend to use the same password across multiple accounts. No wonder 72 percent of people have trouble remembering passwords[8] and 73 percent of online users use the same password all over.[9]

In 2017, 81 percent of hacking-related breaches involved weak or stolen credentials.[2]

Everyone in your ecosystem that uses a password presents a problem. That includes your employees, contractors, vendors, and even your customers. For example, 50 percent of employees don't create different passwords for work and personal accounts.[10] If their personal password is compromised, your organization's data may also be breached.

IT departments often implement password rules—and enforce them with technology—to help ensure strong passwords. The most current recommendations include:

- **Require special characters.** Previously, a mix of numbers and upper and lowercase characters was recommended. But since users usually add numbers to the end of the password and use capital letters at the beginning of words, these patterns actually make passwords easier to predict.

- **Require long passwords.** Password length has the biggest impact, and longer passwords offer greater protection. To help users remember them, suggest that they choose a passphrase, like BrightBlue#25MileRoadM@P.

[8] "5 Obstacles to Employee Productivity," OneLogin.
[9] "TeleSign Consumer Account Security Report," TeleSign.
[10] "Passwords Usage and Human Memory Limitations: A Survey across Age and Educational Background,“ Denise Ranghetti Pilar, Antonio Jaeger, Carlos F. A. Gomes, Lilian Milnitsky Stein, December 2012

- **Require long passwords.** Password length has the biggest impact, and longer passwords offer greater protection. To help users remember them, suggest that they choose a passphrase, like BrightBlue#25MileRoadM@P. •

- **Don't require users to change passwords frequently.** Previously, the recommendation was that users change their passwords every 60 to 90 days, in case a hacker had obtained it. However, that just adds to the memory burden on users, making them more likely to use an easyto-remember password or, worse, to write it on a Post-it Note or in a spreadsheet.

Although stronger passwords help, memory challenges with secure passwords remain a problem. That's why leading-edge organizations realize that the only way to truly close the password security gap is by adding two tools to the IT toolbox—Single Sign-On (SSO) and Multi-Factor Authentication (MFA).

Secure SSO and risk-aware MFA are the golden keys to password security

Single sign-on and multi-factor authentication are critical to truly protecting IP and trade secrets because they address key problems with user authentication:

- Reduce the number of usernames and passwords that employees have to remember.
- Reduce the number of times that employees have to login—even when they need access to multiple apps or websites.
- Require additional information from a user, beyond passwords, to verify the user's identity.
- Make it easy for users to reset their passwords securely if they forget them.

Single sign-on. SSO is a system that lets users securely authenticate with multiple applications and websites by logging in once—with just one set of credentials. With SSO, the applications or websites that users access rely on a trusted third party to verify that users are who they say they are.

Multi-factor authentication. MFA is a security system that verifies a user's identity by requiring multiple credentials. Rather than just asking for a username and password, MFA requires other—additional—credentials, such as a code from the user's smartphone, the answer to a security question, a fingerprint, or facial recognition. (You may have heard MFA referred to by other names, such as two-factor authentication or two-step verification.)

Adding either one of these golden keys will help to lock up your organization's data and prevent unauthorized access. But adding them both will give you the best chance of preventing a breach.

Setting password requirements, enforcing them, and educating users about common attacks make for a good start.

But these aren't nearly enough to protect your corporate or customer data and your IP.

SSO has many benefits

Single sign-on offers multiple benefits, while ensuring that employees only need to sign in once with one set of credentials:

- Greater security and compliance.
- Improved usability and employee satisfaction.
- Lower IT costs.

Security and compliance with SSO are just the beginning

Every time a user logs into a new application or machine, it’s an opportunity for hackers. SSO reduces the number of attack surfaces because employees only login once each day and with only one set of credentials.

SSO helps to address government and industry requirements for effective authentication of users accessing sensitive data. Most SSO systems also provide an audit trail to track user activity and access. And any SSO solution should enable automatic log off, which is another frequent requirement for those working in highly secure environments.

SSO improves usability for employees

Maintaining separate usernames and passwords for each app is a huge burden for your employees. Frankly, it’s unrealistic. And when your employees are at a customer site or a remote location, SSO is even more important.

Single sign-on reduces the cognitive burden on users. Signing in once saves time and frustration, improving employee productivity and satisfaction.

SSO lowers IT costs

Finally, SSO lowers IT costs by reducing password resets. When each app requires a different username and password for every employee, the chances are high that employees will forget passwords, which means that help tickets to reset passwords pile up.

Not only does SSO reduce tickets because users have only one set of credentials to remember, but also it allows people to reset their own passwords, eliminating the need for IT involvement. That’s especially helpful as part of a customer or vendor portal.

Not familiar with SSO?

Find out how it works.

See how SSO helped Mobile Enterprise company SOTI.

How does MFA help security?

MFA has become a widely accepted, critical component of security, because it takes access beyond passwords and requires users to further verify their identity. Those additional factors seriously frustrate hackers in their attempts to obtain login credentials.

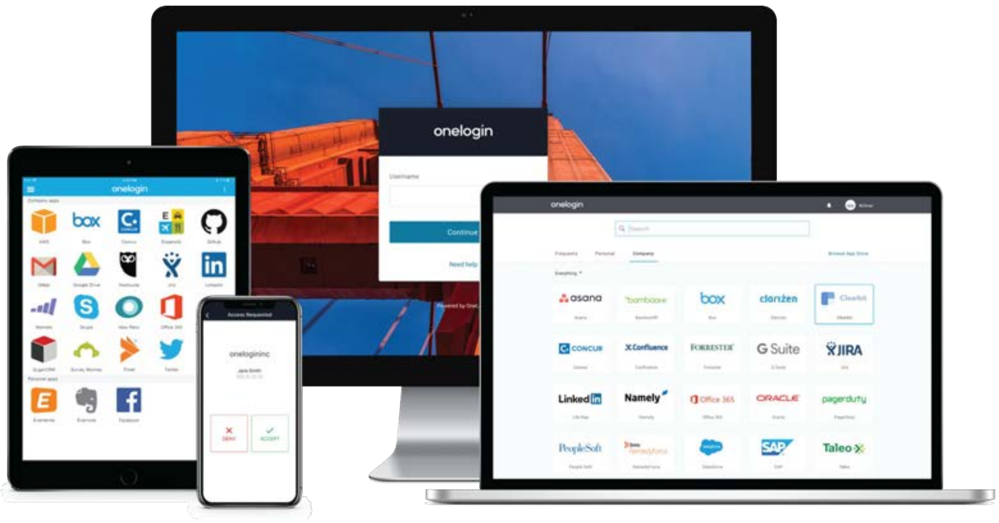
Multi-factor authentication works to prevent successful attacks by requiring additional information or credentials from the user. A phishing attack may garner a user's credentials, but it won't provide the hacker with a fingerprint, for instance, or the answer to a personal security question. Similarly, a brute force or reverse brute force attack may manage to find a working username and password, but the attacker doesn't know which other authentication factors the MFA system will require and, regardless, won't have those credentials.

Similarly, MFA can combat more sophisticated attacks such as MITM by incorporating an additional layer of security. Even if the hacker or program inserts itself and captures the information that an employee or customer enters, you can set up MFA to require that the user supply credentials from a different device or channel. For example, an employee logging in from her laptop may be required to use a phone app, such as OneLogin Protect authenticator, to send a code from the phone to complete the login. The MITM hacker doesn't have access to the user's phone, so the breach is halted.

Not familiar with SSO?

Find out how it works.

See how MFA helped this video game developer.



Devices, devices, so many devices

Your employees and customers aren't just at a desk. They're at home, on the bus, out at customer sites, and in hotels. They're using laptops, tablets, and mobile phones for their work. And they aren't always company devices, either. In a 2016 study, only 20 percent of respondents said they used their personal phones or tablets only for personal use. And in a 2018 study of mobility professionals, 85 percent said they faced at least a moderate risk from mobile security threats.

That's fine. Because both SSO and MFA work across devices. Employees or vendors can sign in—once—from their device to access all the apps they need. It doesn't matter whether they're accessing the information from their phone, tablet, or computer, MFA adapts and asks them for the appropriate additional data to verify their identity.

Adaptive authentication can streamline employee access

SSO certainly offers a more streamlined experience, speeding up and simplifying login. But, since MFA requires that users provide additional information, can it negatively impact employee productivity? The last thing you want to do is slow down employees. Plus, requiring too many authentication factors frustrates users.

That's where adaptive authentication comes in.

Adaptive Authentication add transaction context and user behavior as key authentication factors, taking into consideration how users are trying to access the organization's resources.

Smart authentication systems know how a user normally works, such as where they work from, on which devices, and at what times. Behavior that's considered out of normal for a user can signal an attack. Adaptive MFA responds to the potential attack by requiring additional authentication. 1

Adaptive MFA helps streamline access, keeping employees productive and customers moving forward, because when you implement adaptive authentication in your organization, you determine the baseline login requirements for a given employee or set of employees. You might have stricter requirements for users in certain locales or for users in specific roles and less strict requirements for others.

Each time someone tries to authenticate, the request is evaluated and assigned a risk score. Depending on the risk score, the user may be required to provide additional credentials or, conversely, allowed to use fewer credentials.

So, if an employee is using the laptop he always uses and is attempting to log in from the location where he normally works, he may only be asked to access via his laptop. On the other hand, if the same employee tries to access sensitive and unusual data with his username and password, he may be prompted to enter additional login information on his phone. Or if a manager logs in from a geographical location far from her usual office, she may have to answer a security question.

Learn more about adaptive authentication

Conclusion

IT departments across all industries are in a tough spot when it comes to security. The demands are high, stemming from the bottom line, a constantly-changing workforce, new technologies, and a global ecosystem. But the cost of failure is even higher.

Shoring up some of the weakest links—passwords and authentication—is a relatively fast fix that adds significant protection against breaches. Two technologies are key: single sign-on reduces the attack surface for hackers, and multi-factor authentication adds protection beyond passwords. Adaptive authentication enables organizations to add security in a smart way that doesn't burden employees, customers, vendors, and others. Together, these technologies ensure you can stay agile and productive while still protecting your organization's information.

About OneLogin

OneLogin is the leader in Unified Access Management, Enabling Organizations to Access the World™. Businesses of all sizes use OneLogin to secure company data, while increasing IT administrator and end user efficiencies.

Implementation of our identity management solutions can be achieved in hours rather than days, delivering a fully featured administrative and self-service portal. Our ability to handle on-premises and cloud/ SaaS applications makes us the identity-as-a-service vendor of choice for the hybrid enterprise. Multi-factor authentication, mobile identity management for one-click access on smartphones and tablets, and realtime directory synchronization all add an extra layer of protection.

Contact us to learn more about OneLogin.

www.onelogin.com/company/contact